

Advisor, Identity & Access Management

Role Description:

The Identity & Access Management (IAM) team is responsible for access governance of CUK IT systems and comprises of two functions:

- provisioning and de-provisioning of IT systems access
- performing User Access Reviews (Governance)

The team comprises of IAM analysts (Governance) and IAM Advisors both reporting into the IAM Manager.

The IAM Advisor will be responsible for provisioning and de-provisioning of user access and administrating the joiner, mover and leaver processes. The IAM Advisor should support the governance function and the IAM Analysts in completing the User Access Reviews. The IAM Advisors must understand the controls in place to manage user accounts and work to agreed timelines to meet the agreed service levels. The role demands a good understanding of user administration with good communication and excellent customer service skills.

RUI:	986	Grade:	CUK Level 13	DBS:	Basic
Directorate:	Carnival UK Shared Services	Reports to:	Manager, Identity & Access Management		
Function:	Carnival UK Technology	Team:	Technology Security, Risk & Compliance, Technology Security Operations		
Direct reports :	None				

Accountabilities

- Administer user access and controls within CUK IT system portfolio.
- Provision and de-provision IT system accounts only with an approved service request.
- Onboard new hires using the joiner process and creating accounts when authorised by HR and Line Management.
- Process movers by reaching out to Line Management to confirm changes to access requirements and perform the requested changes.
- Process leavers in a timely manner by disabling/ removing their access when authorised by HR and Line Management.
- Remediate user access compliance activities as a result of UARs.
- Maintain association of IT accounts to individual identities.
- Onboard new systems into the IAM lifecycle and off-board retired systems as required.
- Identify opportunities to streamline IAM processes to meet the requirements of audit and compliance policies.
- Follow, maintain and develop process documentation.
- Participate in internal and external audits to produce evidence of process control.
- Provide support to IAM Compliance team to ensure access control list reports are available when needed.
- Support the continual improvement of tools and technologies in place to support IAM processes.
- Support the IAM Analysts in performing the User Access Reviews and other governance functions.

Health, Environment, Safety, Security (HESS) Responsibilities

- Lead by example by taking care of the health and safety of yourself and others
- Report all accidents, "near miss" incidents and work related ill health conditions to your manager
- Follow safety rules and procedures
- Use work equipment, personal protective equipment, substances and safety devices correctly
- Take part in safety training and risk assessments and suggest ways of reducing risks
- Act in a safe manner in accordance with our safety behaviours

Scope:				
Problem solving: <ul style="list-style-type: none"> Identify technical obstacles and constraints to standardizing IAM controls and suggesting improvements Driving continuous improvement of the effectiveness of control implementations and reporting Impact: <ul style="list-style-type: none"> Improve service performance through knowledge of good practice approach to user access management Meeting compliance target timescales by working diligently to deliver an effective and efficient service Leadership: <ul style="list-style-type: none"> No team management 				
Demonstrable Behaviours (what needs to be demonstrated in 'how' to be successful in the role) :				
<ul style="list-style-type: none"> Guest and customer centric approach, passionate about enhancing the service being offered across the team Natural collaborator, energetic and enthusiastic about cross functional delivery Strong communicator in all Innovator its forms across all levels of the organisation Focussed on prioritising the right things and planning to ensure success Decisive, 'can do' attitude whilst maintaining a clear focus on problem solving and seeing action through to delivery who can develop new ideas and ways to improve the service we offer 				
Skills/competencies required:				
Qualifications – essential: <ul style="list-style-type: none"> None 		Qualifications – desirable: <ul style="list-style-type: none"> Microsoft AD Management ITIL Service Management 		
Knowledge/ Experience – essential: <ul style="list-style-type: none"> In-depth knowledge of Windows Active Directory Management, authentication and group management Knowledge of Identity management principles and standard processes 		Knowledge/ Experience – desirable: <ul style="list-style-type: none"> Use of enterprise class tools to manage IAM and PAM across a large organisation like Sailpoint and Liebermans Experience and good working knowledge of Sarbanes-Oxley, PCI-DSS and related Regulatory policies Experience writing Powershell scripts to help automate IAM processes 		
Issue Date:	June 2019	Issued by:	Sue Still, Manager, Identity & Access Management	
REWARD ONLY	Grade: CUK 13	RUI: 986	Date Approved: 19 June 2019	Initials: LL